UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,848	06/14/2006	Gianluca Cangini	09952.0060	6954

22852 7590 01/07/2009
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
01/07/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/582,848	**Applicant(s)** CANGINI ET AL.	
	Examiner JEFFERY WILLIAMS	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *36-70* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *36-70* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 June 2008* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *61408*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claims 36 – 70 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 37, 39, 44, 46, 47, 49, 54, 56, 61, 63, 64, and 66 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 37, the recitation "all the system primitives that allocate or release said system resources" lacks antecedent basis. For the purpose of examination, the examiner presumes the applicant to recite "system primitives that allocate or release system resources".

Regarding claim 39, the recitation "the file related operations" lacks antecedent basis. For the purpose of examination, the examiner presumes the applicant to recite "file related operations".

Regarding claim 44, the recitation "loosely" is a relative term which renders the claim indefinite. The term "loosely" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. For the purpose of examination, the examiner presumes the applicant to recite "…anomalies matches…".

Regarding claim 46, the recitation "the weight at the previous alert…" lacks antecedent basis. For the purpose of examination, the examiner presumes the applicant to recite "a weight at the previous alert".

Regarding claim 47, the recitation "the common streams of anomalies…" lacks antecedent basis. For the purpose of examination, the examiner presumes the applicant to recite "a common stream of anomalies".

Regarding claim 47, the recitation "the weight associated to the i-th anomaly" lacks antecedent basis. For the purpose of examination, the examiner presumes the applicant to recite "a weight associated to the i-th anomaly".

Regarding claim 49, the recitation "said system watching for changes" lacks antecedent basis. For the purpose of examination, the examiner presumes the applicant to recite "a system watching for changes".

Claims 54, 56, 61, 63, 64, and 66 comprise similar issues as the above claims and are rejected, at least, for the same reasons.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 53 – 70 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Specifically, these claims comprise recitations directed towards software per se (e.g. Specification, pg. 6, line 27 - pg. 7, line 5). As software fails to fall within any of the statutory categories of invention, these claims are rejected as non-statutory.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 36 – 39, 50, 51, 53 – 56, 67, 68, and 70 are rejected under 35 U.S.C. 102(b) as being anticipated by Crosbie, U.S. Patent Publication, 2002/0046275.

Regarding claim 53, Crosbie discloses:

system resources and having a plurality of processes running thereon, comprising analysis modules configured for monitoring, for at least two processes in *said plurality, a set of system primitives that allocate or release said system resources* (Crosbie, fig. 2:210, 220 ,230, 240; par. 114).

Regarding claims 54 and 55, Crosbie discloses:

wherein said analysis modules are configured for monitoring all the system primitives that allocate or release said system resources; wherein said analysis modules are configured for monitoring exclusively those system primitives that allocate or release said system resources (Crosbie, par. 116).

Regarding claim 56, Crosbie discloses:

wherein said analysis modules are selected from the group of: at least one application knowledge module tracking the processes running on said system and monitoring resources used thereby, a network knowledge module monitoring connections by said processes running on said system, a file-system analysis module monitoring the file-related operations performed within said system, and a device monitoring module monitoring operation of commonly used modules with said system (Crosbie, fig. 2:210, 220, 230, 240).

Regarding claim 67, the Crosbie enables:

comprising a plurality of modules for performing said monitoring, said plurality of modules comprising a first set of components depending on the system being monitored *and a second set of components that are independent of the system being monitored* (Crosbie, par. 68; fig. 2:270 vs. 240).

Regarding claim 68, the Crosbie enables:

wherein said first set of modules comprises at least one module selected from the group of: a device driver for intercepting the system calls associated with said primitives in said set; a kernel information module configured for reading information for all processes running on said monitored system; and a system call processor configured for reading the binary data related to the system calls of said system and translating them into respective higher-level system call abstractions (Crosbie, fig. 2:270).

Regarding claims 36 – 39, 50, 51, and 70, they comprise essentially the similar limitations as claims 53 – 56, 67, and 68 and they are rejected, at least, for the same reasons.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 40 – 49, 52, 57 – 66, and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crosbie in view of Ghosh et al. (Ghosh), U.S. Patent 7,181,768.

Regarding claim 57, Crosbie discloses an IDS system employing "misuse detection" wherein system parameters are compared to known templates of intrusive activity (Crosbie, par. 15, 58, 87, 207, 217). However, Crosbie does not appear to explicitly disclose the features of "anomaly detection".

Ghosh discloses that an IDS system may employ both "misuse detection" and "anomaly detection" within the same system (Ghosh, 2:40-44; 2:44-3:8; 4:56-59; 5:15-28).

It would have been obvious to one of ordinary skill in the art to employ teachings of Ghosh within the system of Crosbie. This would have been obvious because one of ordinary skill in the art would have been motivated by an improved system that combines the advantages of each method (e.g. Ghosh, 4:56-59).

Thus the combination enables:

wherein said set of primitives monitored identifies a state of said processing system, comprising a detection component configured for recording a current state of said system over a current period of time and a previous state of the system over a previous period of time, revealing any differences between said current state of the system and said previous state of the system, and detecting any such difference *revealed as a likely anomaly in the system* (Crosbie, par. 192; Ghosh, 6:20-38; 10:56-11:14).

Regarding claim 58, the combination enables:

wherein said detection component is configured for running a learning stage to generate said previous state of the system based on said learning stage (Ghosh, 6:20-38).

Regarding claim 59, the combination enables:

wherein said detection component is configured for correlating a plurality of said anomalies detected and deciding whether these identify a dangerous event for the system (Ghosh, 6:20-38; 10:56-11:14).

Regarding claim 60, the combination enables:

wherein said detection component is configured for emitting an alert signal indicative of any dangerous event for the system identified (Crosbie, par. 84).

Regarding claim 61, the combination enables:

wherein said detection component is configured for: generating a sequence of said anomalies; producing a sequence of pre-conditions in a rule base; and if said sequence of anomalies at least loosely matches said sequence of pre-conditions, issuing a resulting alert signal (Crosbie, par. 84; Ghosh, 11:1-14).

Regarding claim 62, the combination enables:

wherein said detection component is configured for assigning respective weights to said anomalies in said plurality, each said weight being indicative of the criticality of the event represented by the anomaly to which the weight is assigned (Ghosh, 4:63-5:12).

Regarding claim 63, as best understood, the combination enables:

wherein said detection component is configured for associating with each anomaly a value of the weight at the previous alert signal emission time plus the current value modulated with an exponential decay factor, whereby the significance thereof decreases over time (Ghosh, 5:8-14).

Regarding claim 64, the combination enables:

wherein said processing system operates on process identifiers (PID), whereby a plurality of anomalies are detected for the same process identifier, and said detection component is configured for aggregating said anomalies over time according to the following formula: W i + 1 .function. (t) = W i .function. (T i + 1 - T i) + LA i + 1 exp (- t - T i .tau.) W 0 = 0 where W.sub.i is the weight of a user level alert signal associated with the common stream of anomalies, when the i-th anomaly is detected; T.sub.i is the time of detection of the i-th anomaly, LA.sub.i is the weight associated to the i-th anomaly and .tau. is a time-decay constant (Ghosh, 6:27-38; 11:9-14).

Regarding claim 65, the combination enables:

wherein said detection component is configured for correlating said anomalies in said plurality by mapping them into respective fuzzy sets (Ghosh, 4:58; 9:31-44; 8:14-19).

Regarding claim 66, the combination enables:

wherein said monitoring comprises an information gathering component configured for intercepting low-level data within said system watching for changes in the state of the system, thus providing data to be analyzed in said anomaly detection (Crosbie, par, 15).

Regarding claim 69, the combination enables:

comprising a current state module monitoring all processes running on the system monitored and all file descriptors and the socket description used by each said process to produce an instantaneous state of the system monitored (Crosbie, par. 192; Ghosh, 6:20-38; 10:56-11:14).

Regarding claims 40 – 49, 52, they comprise essentially the similar limitations as claims 57 – 66, and 69 and they are rejected, at least, for the same reasons.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

See Notice of References Cited.

A shortened statutory period for reply is set to expire **3** months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

J. Williams
AU 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437